Generalizing Bounds on the Minimum Distance of Cyclic Codes Using Cyclic Product Codes

Alexander Zeh and Antonia Wachter-Zeh
Institute of Communications Engineering
Ulm University, Ulm, Germany
{alex, antonia}@codingtheory.eu

Maximilien Gadouleau
School of Engineering & Computing Sciences (ECS)
Durham University, Durham, UK
m.r.gadouleau@durham.ac.uk

Sergey Bezzateev
Saint Petersburg State University of Airspace Instrumentation
St. Petersburg, Russia
bsv@aanet.ru

***Abstract*—THIS PAPER IS ELIGIBLE FOR THE STUDENT PAPER AWARD**

Two generalizations of the Hartmann–Tzeng (HT) bound on the minimum distance of q-ary cyclic codes are proposed. The first one is proven by embedding the given cyclic code into a cyclic product code. Furthermore, we show that unique decoding up to this bound is always possible and outline a quadratic-time syndrome-based error decoding algorithm. The second bound is stronger and the proof is more involved.

Our technique of embedding the code into a cyclic product code can be applied to other bounds, too and therefore generalizes them.

***Index Terms*—Cyclic Code, Cyclic Product Code, Bound on the Minimum Distance, Efficient Decoding**

I. Introduction

Cyclic codes play a central role in (distributed) storage and communication systems. However, determining their minimum distance from a given defining set is an open research problem. Many lower bounds on the minimum distance and efficient decoding algorithms up to these bounds exist.

In the 1970s, Hartmann and Tzeng (HT, [1], [2]) generalized the well-known bound by Bose, Ray-Chaudhuri [3] and Hocquenghem [4] (BCH). Feng and Tzeng [5], [6] extended the BCH decoding algorithms [7], [8] to decode in quadratic-time up to the HT bound. Further extensions of the BCH bound were *inter alia* developed by Roos [9], [10], van Lint and Wilson [11] (denoted as AB or Shifting method), Duursma and Kötter [12], Boston [13], Duursma and Pellikaan [14] and Betti and Sala [15].

Our first generalization of the HT bound uses the idea of cyclic product codes (see [16]–[18] and Ch. 18 in [19]) and can be applied to other bounds, too. The second approach also associates another cyclic code, but the direct connection to cyclic product codes is not clear.

In contrast to our previous contributions [20], [21] we provide a generalization of the HT bound and show proofs of the statements by means of cyclic product codes.

Our contribution is structured as follows. In Section II, we give necessary preliminaries on cyclic codes, recall the HT bound [1], [2] and provide basic properties of cyclic product codes as they were described first in [16]. The first generalization of the HT bound is proven in Section III and the second one in Section IV. The syndrome-based decoding approach up to the first bound is described in Section V. Section VI concludes our paper.

This work has been supported by DFG, Germany, under grants BO 867/22-1 and BO 867/21-1.

II. Cyclic Codes and Cyclic Product Codes

A. Notation

Let $\mathbb{Z}$ denote the set of integers, $\mathbb{F}_q$ the finite field of order q and $\mathbb{F}_q[X]$ the polynomial ring over $\mathbb{F}_q$ with indeterminate X. A vector of length n is denoted by a lowercase bold letter as $\mathbf{v} = (v_0\, v_1\, \ldots\, v_{n-1})$. An $m \times n$ matrix is denoted by a capital bold letter as $\mathbf{M} = \|m_{i,j}\|_{i=0,j=0}^{m-1,n-1}$. A set is denoted by a capital letter sans serif like D.

A linear $[n,k]_q$ code of length n and dimension k over $\mathbb{F}_q$ is denoted by a calligraphic letter like $\mathcal{C}$ and its minimum Hamming distance by d.

B. Cyclic Codes

An $[n,k]_q$ cyclic code $\mathcal{C}$ with distance d is an ideal in the ring $\mathbb{F}_q[X]/(X^n-1)$ generated by $g(X)$. The generator polynomial $g(X)$ has roots in the splitting field $\mathbb{F}_{q^s}$, where $n \mid (q^s-1)$. The primitive element of order n is α and the defining set $\mathsf{D}_\mathcal{C}$ of an $[n,k]_q$ cyclic code $\mathcal{C}$ is:

$$\mathsf{D}_\mathcal{C} = \big\{0 \le i \le n-1 \,|\, g(\alpha^i) = 0\big\}. \tag{1}$$

Furthermore, we introduce the following short-hand notations for a given $z \in \mathbb{Z}$:

$$\begin{aligned} \mathsf{D}_\mathcal{C}^{[z,\otimes]} &\stackrel{\text{def}}{=} \big\{(i \cdot z) \bmod n \mid i \in \mathsf{D}_\mathcal{C}\big\}, \\ \mathsf{D}_\mathcal{C}^{[z,+]} &\stackrel{\text{def}}{=} \big\{(i + z) \mid i \in \mathsf{D}_\mathcal{C}\big\}. \end{aligned} \tag{2}$$

Let us recall the HT bound [1], [2] and present it in polynomial form, which we use later on.

Theorem 1 (HT Bound [1], [2])**.** *Let an $[n,k]_q$ cyclic code $\mathcal{C}$ with minimum distance d be given and α denotes a primitive element of order n. Assume there exist an integer f and a nonzero integer m with $\gcd(n,m)=1$, such that:*

$$\sum_{i=0}^{\infty} c(\alpha^{f+im+j})X^i \equiv 0 \mod X^{\delta-1} \quad \forall j = 0,\ldots,\nu, \tag{3}$$

holds for all $c(x) \in \mathcal{C}$ and some integers $\delta \geq 2$ and $\nu \geq 0$.

Then, $d \geq \delta + \nu$.

Note that for $\nu = 0$, the HT bound becomes the BCH bound [3], [4].

Let $\mathcal{A}$ and $\mathcal{B}$ be $[n_1, k_1]_q$ and $[n_2, k_2]_q$ linear codes over $\mathbb{F}_q$ with minimum Hamming distance d_1 and d_2. For simplicity, we assume that the first $k_1|k_2$ symbols are the information symbols of $\mathcal{A}|\mathcal{B}$.

Definition 1 (Product Code)**.** *The direct product $\mathcal{A} \otimes \mathcal{B}$ is an $[n_1 n_2, k_1 k_2]_q$ code with distance $d_1 d_2$ which consists of all $n_1 \times n_2$ matrices whose rows are all codewords of $\mathcal{A}$ and whose columns are all codewords of $\mathcal{B}$.*

We recall Thm. 1 of Burton and Weldon [16]. Throughout the paper, we restrict ourselves to the case where both codes are over the same alphabet.

Theorem 2 (Cyclic Product Code)**.** *Let an $[n_1, k_1]_q$ cyclic code $\mathcal{A}$ with minimum distance d_1 and a second $[n_2, k_2]_q$ cyclic code $\mathcal{B}$ with minimum distance d_2 be given. The product code $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is an $[n_1 n_2, k_1 k_2]_q$ cyclic code (with distance $d = d_1 d_2$) provided that the two lengths n_1 and n_2 are relatively prime, i.e., $an_1 + bn_2 = 1$ for some integers a and b. Let the $n_1 \times n_2$ matrix $\mathbf{M} = \|m_{i,j}\|_{i=0,j=0}^{n_1-1,n_2-1}$ be a codeword of $\mathcal{C}$ (as in Def. 1). Then, the univariate polynomial $c(X) = \sum_{i=0}^{n_1 n_2 - 1} c_i X^i \in \mathbb{F}_q[X]$ with*

$$c_i = m_{i \bmod n_1, i \bmod n_2} \quad \forall i = 0, 1, \ldots, n_1 n_2 - 1 \tag{4}$$

is a codeword of the cyclic product code $\mathcal{C}$ that is an ideal in the ring $\mathbb{F}_q[X]/(X^{n_1 n_2} - 1)$.

Let us outline how the defining set $\mathsf{D}_\mathcal{C}$ of $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ can be obtained from $\mathsf{D}_\mathcal{A}$ and $\mathsf{D}_\mathcal{B}$. We summarize the results of Lin and Weldon [18], Thm. 4.

Theorem 3 (Defining Set and Generator Polynomial of a Cyclic Product Code)**.** *Let $\mathcal{A}$ and $\mathcal{B}$, respectively $[n_1, k_1]_q$ and $[n_2, k_2]_q$, be cyclic codes with defining sets $\mathsf{D}_\mathcal{A}$ and $\mathsf{D}_\mathcal{B}$ and generator polynomials $g_1(X)$ and $g_2(X)$. Let $an_1 + bn_2 = 1$ for some integers a and b. Then, the generator polynomial $g(X)$ of the cyclic product code $\mathcal{A} \otimes \mathcal{B}$ is:*

$$g(X) = \gcd\Big(X^{n_1 n_2} - 1, g_1(X^{bn_2}) \cdot g_2(X^{an_1})\Big). \tag{5}$$

Let $\mathsf{B}_\mathcal{A} = \mathsf{D}_\mathcal{A}^{[b,\otimes]}$ and let $\mathsf{A}_\mathcal{B} = \mathsf{D}_\mathcal{B}^{[a,\otimes]}$ as given in (2)*. The defining set of the cyclic product code $\mathcal{C}$ is:*

$$\mathsf{D}_\mathcal{C} = \left\{ \left\{ \bigcup_{i=0}^{n_2-1} \mathsf{B}_\mathcal{A}^{[in_1,+]} \right\} \cup \left\{ \bigcup_{i=0}^{n_1-1} \mathsf{A}_\mathcal{B}^{[in_2,+]} \right\} \right\}.$$

Let us restate Thm. 2 of [21] on the minimum distance of cyclic codes using cyclic product codes.

Theorem 4 (BCH Bound Generalization)**.** *Let an $[n_1, k_1]_q$ cyclic code $\mathcal{A}$ with minimum distance d_1 and a second $[n_2, k_2]_q$ cyclic code $\mathcal{B}$ with minimum distance d_2 and with $\gcd(n_1, n_2) = 1$ be given. Let α be a primitive element of order n_1 in $\mathbb{F}_{q^{s_1}}$, β of order n_2 in $\mathbb{F}_{q^{s_2}}$ respectively and let two integers f_1, f_2 and two nonzero integers m_1,m_2 with $\gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$ be given. For all codewords $a(X) \in \mathcal{A}$ and $b(X) \in \mathcal{B}$*

$$\sum_{i=0}^{\infty} a(\alpha^{f_1 + im_1}) \cdot b(\beta^{f_2 + im_2}) X^i \equiv 0 \mod X^{\delta - 1} \tag{6}$$

holds for some integer $\delta \geq 2$. Then, we obtain:

$$d_1 \geq d^* = \left\lceil \frac{\delta}{d_2} \right\rceil. \tag{7}$$

Note that the expression of (6) is in $\mathbb{F}_{q^s}[X]$, where $s = \operatorname{lcm}(s_1, s_2)$.

Proof: From Thm. 3 we know that (6) corresponds to $\delta - 1$ consecutive zeros in the defining set $\mathsf{D}_\mathcal{C}$ of $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ and therefore its distance $d = d_1 d_2$ is greater than or equal to δ. ∎

Moreover, this yields the following explicit relation.

Proposition 1 (BCH Bound of the Cyclic Product Code)**.** *Let the integers $f_1, f_2, m_1 \neq 0, m_2 \neq 0$ and $\delta \geq 2$ and two cyclic codes $\mathcal{A}$ and $\mathcal{B}$ with $an_1 + bn_2 = 1$ be given as in Thm. 4. Then, the two integers:*

$$\begin{aligned} f &= f_1 \cdot b^2 n_2 + f_2 \cdot a^2 n_1 \qquad \text{and} \\ m &= m_1 \cdot b^2 n_2 + m_2 \cdot a^2 n_1 \end{aligned}$$

denote the parameters such that:

$$\sum_{i=0}^{\infty} c(\gamma^{f + im}) X^i \equiv 0 \mod X^{\delta - 1} \tag{8}$$

holds for all $c(X) \in \mathcal{A} \otimes \mathcal{B}$, where γ is a primitive element of order $n_1 n_2$ in $\mathbb{F}_{q^s}[X]$.

Proof: Let $g_1(X)$ be the generator polynomial of $\mathcal{A}$ and $g_2(X)$ that of $\mathcal{B}$. From Thm. 3 we know that if α^i is a root of $g_1(X)$, then γ^{bi} is a root of $g(X)$ as in (5) and γ^{ai} is a root of $g(X)$ if β^i is a root of $g_2(X)$. Therefore we want $f + im \equiv b(f_1 + im_1) \bmod n_1$ and $f + im \equiv a(f_2 + im_2) \bmod n_2$ and the Chinese-Remainder-Theorem gives the result. ∎

Example 1 (BCH Bound of the Cyclic Product Code)**.** *Let $\mathcal{A}$ be the binary reversible $[17, 9]_2$ code with $\mathsf{D}_\mathcal{A} = \{1, 2, 4, 8, -8, -4, -2, -1\}$ and let $\mathcal{B}$ denote the binary $[3, 2]_2$ single parity check code with $\mathsf{D}_\mathcal{B} = \{0\}$. Let $\alpha \in \mathbb{F}_{2^8}$ and $\beta \in \mathbb{F}_{2^4}$ denote elements of order 17 and 3, respectively. Then, we know that for $f_1 = -4$, $f_2 = -1$ and $m_1 = m_2 = 1$ Thm. 4 holds for $\delta = 10$ and therefore $d_1 \geq 5$, which is the true minimum distance of $\mathcal{A}$.*

Since $-1 \cdot 17 + 6 \cdot 3 = 1$, according to Thm. 3 the defining set of the cyclic product code $\mathcal{A} \otimes \mathcal{B}$ is $\mathsf{D}_{\mathcal{A} \otimes \mathcal{B}}$:

$$\begin{aligned} =&\Big\{\{3, 5, 6, 7, 10, 11, 12, 14\} \cup \{20, 22, 23, 24, 27, 28, 29, 31\} \\ &\cup \{37, 39, 40, 41, 44, 45, 46, 48\} \cup \{0\} \cup \{3\} \cup \cdots \cup \{48\}\Big\} \\ =&\{0, 3, 5, 6, 7, 9, 11, 12, 14, 15, 18, 20, 21, 22, 23, 24, 27, 28, \\ &\qquad 29, 30, 31, 33, 36, 37, 39, 40, 41, 42, 44, 45, 46, 48\} \end{aligned}$$

and Proposition 1 gives $f = 22$ and $m = 20$.

III. Generalized HT Bound I: Using Cyclic Product Code

In this section, we consider the first generalization of Thm. 4.

Theorem 5 (Generalized HT Bound I)**.** *Let an $[n_1, k_1]_q$ cyclic code $\mathcal{A}$ with minimum distance d_1 and a second $[n_2, k_2]_q$ cyclic code $\mathcal{B}$ with minimum distance d_2 and $\gcd(n_1, n_2) = 1$ be given. Let α be a primitive element of order n_1 in $\mathbb{F}_{q^{s_1}}$, β of order n_2 in $\mathbb{F}_{q^{s_2}}$, respectively, and let two integers f_1 and f_2 and two nonzero integers m_1 and m_2 with $\gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$ be given. For all codewords $a(X) \in \mathcal{A}$ and $b(X) \in \mathcal{B}$*

$$\sum_{i=0}^{\infty} a(\alpha^{f_1+im_1+j}) \cdot b(\beta^{f_2+im_2+j}) X^i \equiv 0 \bmod X^{\delta-1} \quad \forall j = 0, \ldots, \nu \tag{9}$$

holds for some integers $\delta \geq 2$ and $\nu \geq 0$. Then, the minimum distance d_1 of $\mathcal{A}$ is lower bounded by:

$$d_1 \geq d^{**} \stackrel{\text{def}}{=} \left\lceil \frac{\delta + \nu}{d_2} \right\rceil. \tag{10}$$

Proof: From the generator polynomial of the cyclic product code $\mathcal{A} \otimes \mathcal{B}$ (see Thm. 3) we know that whenever $a(X) \in \mathcal{A}$ or $b(X) \in \mathcal{B}$ have a zero, then a codeword of the cyclic product code $\mathcal{A} \otimes \mathcal{B}$ is also zero at the evaluated point (as stated in Lemma 1). Therefore, $\delta + \nu$ is the HT bound (see Thm. 1) of $\mathcal{A} \otimes \mathcal{B}$ and $d_1 d_2 \geq \delta + \nu$. ∎

IV. Generalized HT Bound II: Using a Second Cyclic Code

In this section, we consider the second generalization of Thm. 4 and the proof of the statement is more involved.

Theorem 6 (Generalized HT Bound II)**.** *Let an $[n_1, k_1]_q$ cyclic code $\mathcal{A}$ with minimum distance d_1 and a second $[n_2, k_2]_q$ cyclic code $\mathcal{B}$ with minimum distance d_2 and with $\gcd(n_1, n_2) = 1$ be given. Let α be a primitive element of order n_1 in $\mathbb{F}_{q^{s_1}}$, β of order n_2 in $\mathbb{F}_{q^{s_2}}$ respectively and let two integers f_1 and f_2 and two nonzero integers m_1 and m_2 with $\gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$ be given. For all codewords $a(X) \in \mathcal{A}$ and $b(X) \in \mathcal{B}$*

$$\sum_{i=0}^{\infty} a(\alpha^{f_1+im_1+j}) \cdot b(\beta^{f_2+im_2}) X^i \equiv 0 \bmod X^{\delta-1} \quad \forall j = 0, \ldots, \nu \tag{11}$$

holds for some integers $\delta \geq 2$ and $\nu \geq 0$. Then, the minimum distance d_1 of $\mathcal{A}$ is lower bounded by:

$$d_1 \geq d^{***} \stackrel{\text{def}}{=} \left\lceil \frac{\delta}{d_2} + \nu \right\rceil. \tag{12}$$

Proof: Let $a(X) = \sum_{i \in \mathsf{Y}} a_i X^i$ with $\mathsf{Y} = \{i_1, i_2, \ldots, i_y\}$ and $b(X) = \sum_{i \in \mathsf{Z}} b_i X^i$ with $\mathsf{Z} = \{j_1, j_2, \ldots, j_z\}$. We combine the $\nu + 1$ sequences (multiplying each of it by $\lambda_i \in \mathbb{F}_{q^s}$, $s = \operatorname{lcm}(s_1, s_2)$) and obtain:

$$\sum_{i=0}^{\infty} \Bigg(\lambda_0 \sum_{\ell \in \mathsf{Z}} b_\ell \beta^{\ell(f_2+im_2)} (a_{i_1} \alpha^{i_1(f_1+im_1)} + \cdots + a_{i_y} \alpha^{i_y(f_1+im_1)}) + \lambda_1 \sum_{\ell \in \mathsf{Z}} b_\ell \beta^{\ell(f_2+im_2)} (a_{i_1} \alpha^{i_1(f_1+im_1+1)} + \ldots + a_{i_y} \alpha^{i_y(f_1+im_1+1)}) + \cdots + \lambda_\nu \sum_{\ell \in \mathsf{Z}} b_\ell \beta^{\ell(f_2+im_2)} (a_{i_1} \alpha^{i_1(f_1+im_1+\nu)} + \cdots + a_{i_y} \alpha^{i_y(f_1+im_1+\nu)}) X^i \equiv 0 \bmod X^{\delta-1}.$$

Simplified, this result in:

$$\sum_{i=0}^{\infty} b(\beta^{f_2+im_2}) \Big(\sum_{\ell \in \mathsf{Y}} a_\ell \alpha^{\ell(f_1+im_1)} (\lambda_0 + \alpha^\ell \lambda_1 + \ldots + \alpha^{\ell\nu} \lambda_\nu) \Big) X^i \equiv 0 \mod X^{\delta-1}. \tag{13}$$

We want to annihilate the first ν terms and guarantee that the linear combination is nonzero. The corresponding $(\nu+1) \times (\nu+1)$ system of equations:

$$\begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{i_1 2} & \cdots & \alpha^{i_1 \nu} \\ 1 & \alpha^{i_2} & \alpha^{i_2 2} & \cdots & \alpha^{i_2 \nu} \\ & & \vdots & & \\ 1 & \alpha^{i_{\nu+1}} & \alpha^{i_{\nu+1} 2} & \cdots & \alpha^{i_{\nu+1} \nu} \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_\nu \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{14}$$

has a unique nonzero solution due to full rank of the square Vandermonde matrix of order $\nu + 1$ generated by the distinct elements $\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{\nu+1}}$.

Let $\widetilde{\mathsf{Y}} \stackrel{\text{def}}{=} \mathsf{Y} \setminus \{i_1, i_2, \ldots, i_\nu\}$ and (13) leads to:

$$\sum_{i=0}^{\infty} b(\beta^{f_2+im_2}) \Big(\sum_{\ell \in \widetilde{\mathsf{Y}}} a_i \alpha^{\ell(f_1+im_1)} (\lambda_0 + \alpha^\ell \lambda_1 + \cdots + \alpha^{\ell\nu} \lambda_\nu) \Big) X^i \equiv 0 \mod X^{\delta-1}.$$

This leads to (for the sake of clarity, we let $m_1 = m_2 = 1$):

$$\frac{\sum_{i \in \widetilde{\mathsf{Y}}} \Big(a_i \alpha^{if_1} \sum_{j \in \mathsf{Z}} \Big(b_j \beta^{jf_2} \prod_{\substack{\ell \in \mathsf{Z} \\ \ell \neq j}} (1 - X\alpha^i \beta^\ell) \Big) \prod_{\substack{h \in \widetilde{\mathsf{Y}} \\ h \neq i}} \prod_{p \in \mathsf{Z}} (1 - X\alpha^h \beta^p) \Big)}{\prod_{i \in \widetilde{\mathsf{Y}}} \big(\prod_{j \in \mathsf{Z}} (1 - X\alpha^i \beta^j) \big)} \equiv 0 \mod X^{\delta-1},$$

where the numerator is a nonzero linear combination of the polynomials $\prod_{(h,l) \neq (i,j)} (1 - X\alpha^h \beta^l)$. It is easily shown that all of those polynomials are distinct and linearly independent (it requires that $\gcd(n_1, n_2) = \gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$). Hence, the numerator is a nonzero polynomial. Its degree is smaller than or equal to $z - 1 + z(y - \nu - 1) = z(y - \nu) - 1$ and therefore with $d_1 \geq y$ and $d_2 \geq z$, the statement follows. ∎

V. Decoding up to Generalized HT Bound I

Let $r(X) = a(X) + e(X)$ be the received polynomial, where $e(X) = \sum_{i \in E} e_i x^i \in \mathbb{F}_q[X]$ is the error word and $\mathsf{E} = \{j_1, j_2, \ldots, j_t\} \subseteq \{0, \ldots, n_1 - 1\}$ is the set of error

positions of cardinality $|\mathsf{E}| = t$ and $a(X)$ is a codeword of a given $[n_1, k_1]_q$ code $\mathcal{A}$.

We describe how to decode up to the generalized bound from Thm. 5. Therefore, we want to decode $t \leq \tau$ errors, where

$$\tau \leq \frac{d^{**} - 1}{2} = \frac{\delta + \nu - 1}{2d_2}. \tag{15}$$

Let $b(X) \in \mathcal{B}$ be of weight d_2 and $\alpha \in \mathbb{F}_{q^{s_1}}$, $\beta \in \mathbb{F}_{q^{s_2}}$ and the integers $f_1, f_2, m_1 \neq 0, m_2 \neq 0$ be given such that Thm. 5 for δ and ν holds. Denote $s = \mathrm{lcm}(s_1, s_2)$. We define $\nu + 1$ syndrome polynomials $S^{(j)}(X) \in \mathbb{F}_{q^s}[X]$ for $j = 0, \ldots, \nu$ as follows:

$$\begin{aligned} S^{(j)}(X) &\stackrel{\text{def}}{=} \sum_{i=0}^{\infty} r(\alpha^{f_1 + im_1 + j}) \cdot b(\beta^{f_2 + im_2 + j}) X^i \bmod X^{\delta - 1} \\ &= \sum_{i=0}^{\delta - 2} e(\alpha^{f_1 + im_1 + j}) \cdot b(\beta^{f_2 + im_2 + j}) X^i. \end{aligned} \tag{16}$$

This generalizes our previous approach [20] to $\nu+1$ syndrome sequences of length $\delta-1$. Hence, we obtain $\nu+1$ key equations with a common error-locator polynomial $\Lambda(X) \in \mathbb{F}_{q^s}[X]$ of degree $d_2 t$ (compare also [20], Equation (20)):

$$\Omega^{(j)}(X) \equiv \Lambda(X) \cdot S^{(j)}(X) \bmod X^{\delta - 1}, \quad j = 0, \ldots, \nu,$$

where the degree of $\Omega^{(j)}(X)$ is less than $d_2 t$. Solving these $\nu + 1$ key equations jointly is a multi-sequence shift-register synthesis problem for sequences of equal length; for efficient algorithms see e.g. Feng–Tzeng [5], [6].

The basic task is to solve the following linear system of equations for $\Lambda(X) = \Lambda_0 + \Lambda_1 X + \cdots + \Lambda_{d_2 t} X^{d_2 t}$, which we normalized such that $\Lambda_0 = 1$:

$$\begin{pmatrix} \mathbf{S}^{(0)} \\ \mathbf{S}^{(1)} \\ \vdots \\ \mathbf{S}^{(\nu)} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_{d_2 t} \\ \vdots \\ \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} \mathbf{T}^{(0)} \\ \mathbf{T}^{(1)} \\ \vdots \\ \mathbf{T}^{(\nu)} \end{pmatrix}, \tag{17}$$

where each sub-matrix $\mathbf{S}^{(j)}$ is a $(\delta - 1 - d_2 t) \times (d_2 t)$ matrix and $\mathbf{T}^{(j)}$ is a column vector of length $\delta - 1 - d_2 t$ as follows:

$$\mathbf{S}^{(j)} = \begin{pmatrix} S_0^{(j)} & S_1^{(j)} & \ldots & S_{d_2 t - 1}^{(j)} \\ S_1^{(j)} & S_2^{(j)} & \ldots & S_{d_2 t}^{(j)} \\ \vdots & & & \vdots \\ S_{\delta - 2 - d_2 t}^{(j)} & S_{\delta - 1 - d_2 t}^{(j)} & \ldots & S_{\delta - 3}^{(j)} \end{pmatrix} \tag{18}$$

and $\mathbf{T}^{(j)} = (S_{d_2 t}^{(j)}, S_{d_2 t + 1}^{(j)}, \ldots, S_{\delta - 2}^{(j)})^T$. In the following, denote $\mathbf{S} \stackrel{\text{def}}{=} (\mathbf{S}^{(0)T}, \mathbf{S}^{(1)T}, \ldots, \mathbf{S}^{(\nu)T})^T$. In order to guarantee unique decoding, we have to prove that the syndrome matrix $\mathbf{S}$ from (17) has full rank if (15) is fulfilled. For simplicity, we consider only a single parity check code for $\mathcal{B}$ with $d_2 = 2$.

Theorem 7 (Decoding up to Generalized HT Bound I for a single parity check code with $d_2 = 2$)**.** *Let $\mathcal{B}$ be a single parity check code with $d_2 = 2$ and let $\gcd(n_1, n_2) = \gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$ hold. Moreover, let* (15) *be fulfilled and let $\nu+1$ syndrome sequences of length $\delta-1$ be defined as in* (16)*. Then, the syndrome matrix $\mathbf{S}$ with the submatrices from* (18) *has $\mathrm{rank}(\mathbf{S}) = 2t$.*

Proof: Let us w.l.o.g. assume that $b(X) = 1 + X$ and $f_1 = f_2 = 0$. Then, the $\nu + 1$ syndrome polynomials in $\mathbb{F}_{q^s}[X]$ are $S^{(j)}(X) = \sum_{i=0}^{\delta - 2} e(\alpha^{im_1 + j})(1 + \beta^{im_2 + j}) X^i$ for $j = 0, 1, \ldots, \nu$. Similar to [6], Section VI, we can decompose the syndrome matrix into three matrices as follows.

$$\mathbf{S} = \begin{pmatrix} \mathbf{S}^{(0)} \\ \vdots \\ \mathbf{S}^{(\nu)} \end{pmatrix} = \mathbf{X} \cdot \mathbf{Y} \cdot \overline{\mathbf{X}} = \begin{pmatrix} \mathbf{X}^{(0)} \\ \vdots \\ \mathbf{X}^{(\nu)} \end{pmatrix} \cdot \mathbf{Y} \cdot \overline{\mathbf{X}},$$

where $\mathbf{X}$ is a $(\nu + 1)(\delta - 1 - 2t) \times 2t$ matrix over $\mathbb{F}_{q^s}$ and $\mathbf{Y}$ and $\overline{\mathbf{X}}$ are $2t \times 2t$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^s}$, respectively. The decomposition provides the following matrices with $\kappa = \delta - 2 - 2t$:

$$\mathbf{X}^{(j)} = \begin{pmatrix} \begin{pmatrix} \alpha^{j_1 j} & \ldots & \alpha^{j_t j} \\ \alpha^{j_1 (j + m_1)} & \ldots & \alpha^{j_t (j + m_1)} \\ \vdots & & \vdots \\ \alpha^{j_1 (j + m_1(\kappa))} & \ldots & \alpha^{j_t (j + m_1(\kappa))} \end{pmatrix} \\ \begin{pmatrix} \beta^j \alpha^{j_1 j} & \ldots & \beta^j \alpha^{j_t j} \\ \beta^{j + m_2} \alpha^{j_1 (j + m_1)} & \ldots & \beta^{j + m_2} \alpha^{j_t (j + m_1)} \\ \vdots & & \vdots \\ \beta^{j + m_2(\kappa) t} \alpha^{j_1 (j + m_1(\kappa))} & \ldots & \beta^{j + m_2(\kappa)} \alpha^{j_t (j + m_1(\kappa))} \end{pmatrix} \end{pmatrix},$$

and $\mathbf{Y} = \mathrm{diag}(e_{j_1}, e_{j_2}, \ldots, e_{j_t}, e_{j_1}, e_{j_2}, \ldots, e_{j_t})$ and

$$\overline{\mathbf{X}} = \left(\begin{array}{cccc} 1 & \alpha^{j_1 m_1} & \ldots & \alpha^{j_1 m_1 (2t-1)} \\ 1 & \alpha^{j_2 m_1} & \ldots & \alpha^{j_2 m_1 (2t-1)} \\ & \vdots & & \vdots \\ 1 & \alpha^{j_t m_1} & \ldots & \alpha^{j_t m_1 (2t-1)} \\ \hline 1 & \beta^{m_2} \alpha^{j_1 m_1} & \ldots & (\beta^{m_2} \alpha^{j_1 m_1})^{(2t-1)} \\ 1 & \beta^{m_2} \alpha^{j_2 m_1} & \ldots & (\beta^{m_2} \alpha^{j_2 m_1})^{(2t-1)} \\ & \vdots & & \vdots \\ 1 & \beta^{m_2} \alpha^{j_t m_1} & \ldots & (\beta^{m_2} \alpha^{j_t m_1})^{(2t-1)} \end{array}\right).$$

Since $\mathbf{Y}$ is a diagonal matrix, it is non-singular. From $\gcd(n_1, n_2) = \gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$ we know that $\overline{\mathbf{X}}$ is a Vandermonde matrix and has full rank. Hence, $\mathbf{Y} \cdot \overline{\mathbf{X}}$ is a non-singluar $2t \times 2t$ matrix and therefore $\mathrm{rank}(\mathbf{S}) = \mathrm{rank}(\mathbf{X})$. In order to analyze the rank of $\mathbf{X}$, we proceed similarly as in [6], Sec. VI. We use the matrix operation from [11] (see Corollary 1 in the appendix) to rewrite $\mathbf{X} = \mathbf{A} * \mathbf{B}$, where

$$\mathbf{A} = \begin{pmatrix} 1 & \ldots & 1 & 1 & \ldots & 1 \\ \alpha^{j_1} & \ldots & \alpha^{j_t} & \beta \alpha^{j_1} & \ldots & \beta \alpha^{j_t} \\ \vdots & & & & & \vdots \\ \alpha^{j_1 \nu} & \ldots & \alpha^{j_t \nu} & (\beta \alpha^{j_1})^{\nu} & \ldots & (\beta \alpha^{j_t})^{\nu} \end{pmatrix}$$

and $\mathbf{B} = \mathbf{X}^{(0)}$.

Since $\gcd(n_1, n_2) = \gcd(n_1, m_1) = \gcd(n_2, m_2) = 1$, both matrices $\mathbf{A}$ and $\mathbf{B}$ are Vandermonde matrices with ranks:

$$\mathrm{rank}(\mathbf{A}) = \min\{\nu + 1, 2t\}, \ \mathrm{rank}(\mathbf{B}) = \min\{\delta - 1 - 2t, 2t\}.$$

Note that w.l.o.g. we can always define m_1, m_2, δ and ν such that $\nu + 1 \leq \delta - 1$. Therefore, from (15) we obtain:

$$t \leq \frac{d^{**} - 1}{2} = \frac{\delta + \nu - 1}{2d_2} \leq \frac{2(\delta - 1) - 1}{2d_2} < \frac{\delta - 1}{d_2}. \quad (19)$$

Hence, investigating all possible four cases of $\mathrm{rank}(\mathbf{A}) + \mathrm{rank}(\mathbf{B})$ gives:

$$\begin{aligned} &2t + 2t = 4t > 2t, \\ &2t + \nu + 1 > 2t, \\ &\delta - 1 - 2t + 2t = \delta - 1 > 2t, \\ &\delta - 1 - 2t + \nu + 1 \geq 2d_2 t - 2t + 1 = 2t + 1 > 2t, \end{aligned}$$

where the last two above inequalities used (19) and $d_2 = 2$. Thus, $\mathrm{rank}(\mathbf{A}) + \mathrm{rank}(\mathbf{B}) > 2t$. With Corollary 1 in the appendix, we have proven the statement. ∎

Therefore, the joint key equation (17) has a unique solution, which can be found by multi-sequence shift-register synthesis with $\mathcal{O}(sn^2)$ operations over $\mathbb{F}_{q^s}$ [5], [6]. The extension of the proof for decoding up to $t \leq \tau$ errors as in (15) to other associated codes $\mathcal{B}$ with $d_2 \geq 2$ is straight-forward. The decomposition of the syndrome matrix $\mathbf{S}$ can be done similarly and we can prove that it has rank $d_2 t$. The details of the root-finding of $\Lambda(X)$ to obtain the error-locations and the determination of the error-values can be found in Sec. 6 of [21].

VI. Conclusion

We presented two techniques to generalize the HT bound on the minimum Hamming distance of q-ary cyclic codes. The first one is directly related to cyclic product codes and facilitates a syndrome-based algebraic decoding algorithm. The second approach's connection to product codes is an open topic as well as a decoding approach up to this bound.

Probably, it is possible to generalize other bounds (Roos, van Lint–Wilson) on the minimum distance of cyclic codes by embedding the given code into a cyclic product code. Furthermore, it seems possible to apply this approach similarly to the wider class of linear codes.

Acknowledgments

The authors are grateful to Daniel Augot for stimulating discussions.

Appendix

The following corollary follows directly from Thm. 4 [11].

Corollary 1 (vLW-Matrix Product and Rank)**.** *Let the following matrix operation be defined as in [11]:*

$$\mathbf{X} = \mathbf{A} * \mathbf{B} = \begin{pmatrix} a_{1,1}\mathbf{b}_1 & a_{1,2}\mathbf{b}_2 & \dots & a_{1,2t}\mathbf{b}_{2t} \\ a_{2,1}\mathbf{b}_1 & a_{2,2}\mathbf{b}_2 & \dots & a_{2,2t}\mathbf{b}_{2t} \\ \vdots & & & \vdots \\ a_{\nu+1,1}\mathbf{b}_1 & a_{\nu+1,2}\mathbf{b}_2 & \dots & a_{\nu+1,2t}\mathbf{b}_{2t} \end{pmatrix},$$

where $\mathbf{A}$ *is a* $(\nu + 1) \times 2t$ *matrix,* $\mathbf{B}$ *is a* $(\delta - 1 - 2t) \times 2t$ *matrix and* $\mathbf{b}_i$ *denotes the* i*-th column of* $\mathbf{B}$*, and* $\mathbf{X}$ *has* $2t$ *columns. If* $\mathrm{rank}(\mathbf{A}) + \mathrm{rank}(\mathbf{B}) > 2t$*, then* $\mathrm{rank}(\mathbf{X}) = 2t$*.*

References

[1] C. Hartmann, "Decoding Beyond the BCH Bound", *IEEE Transactions on Information Theory*, vol. 18, no. 3, pp. 441–444, May 1972. DOI: 10.1109/TIT.1972.1054824.

[2] C. Hartmann and K. Tzeng, "Generalizations of the BCH Bound", *Information and Control*, vol. 20, no. 5, pp. 489–498, Jun. 1972. DOI: 10.1016/S0019-9958(72)90887-X.

[3] R. C. Bose and D. K. R. Chaudhuri, "On A Class of Error Correcting Binary Group Codes", *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960. DOI: 10.1016/S0019-9958(60)90287-4.

[4] A. Hocquenghem, "Codes Correcteurs d'Erreurs", *Chiffres (Paris)*, vol. 2, pp. 147–156, Sep. 1959.

[5] G.-L. Feng and K. Tzeng, "A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis", *IEEE Transactions on Information Theory*, vol. 35, no. 3, pp. 584–594, May 1989. DOI: 10.1109/18.30981.

[6] ——, "A Generalization of the Berlekamp–Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes", *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1274–1287, 1991. DOI: 10.1109/18.133246.

[7] J. Massey, "Shift-Register Synthesis and BCH Decoding", *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969. DOI: 10.1109/TIT.1969.1054260.

[8] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A Method for Solving Key Equation for Decoding Goppa Codes", *Information and Control*, vol. 27, no. 1, pp. 87–99, Jan. 1975. DOI: 10.1016/S0019-9958(75)90090-X.

[9] C. Roos, "A Generalization of the BCH Bound for Cyclic Codes, Including the Hartmann-Tzeng Bound", *Journal of Combinatorial Theory, Series A*, vol. 33, no. 2, pp. 229–232, Sep. 1982. DOI: 10.1016/0097-3165(82)90014-0.

[10] ——, "A New Lower Bound for the Minimum Distance of a Cyclic Code", *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 330–332, May 1983. DOI: 10.1109/TIT.1983.1056672.

[11] J. van Lint and R. Wilson, "On The Minimum Distance of Cyclic Codes", *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 23–40, Jan. 1986. DOI: 10.1109/TIT.1986.1057134.

[12] I. M. Duursma and R. Kötter, "Error-Locating Pairs for Cyclic Codes", *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1108–1121, Jul. 1994. DOI: 10.1109/18.335964.

[13] N. Boston, "Bounding Minimum Distances of Cyclic Codes Using Algebraic Geometry", *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 385–394, 2001. DOI: 10.1016/S1571-0653(04)00190-8.

[14] I. M. Duursma and R. Pellikaan, "A Symmetric Roos Bound for Linear Codes", *Journal of Combinatorial Theory Series A - Special Issue in Honor of J. H. van Lint*, vol. 113, pp. 1677–1688, 2006. DOI: 10.1016/j.jcta.2006.03.020.

[15] E. Betti and M. Sala, "A New Bound for the Minimum Distance of a Cyclic Code From Its Defining Set", *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3700–3706, Aug. 2006. DOI: 10.1109/TIT.2006.876240.

[16] H. Burton and E. Weldon, "Cyclic Product Codes", *IEEE Transactions on Information Theory*, vol. 11, no. 3, pp. 433–439, Jul. 1965. DOI: 10.1109/TIT.1965.1053802.

[17] N. Abramson, "Cascade Decoding of Cyclic Product Codes", *IEEE Transactions on Communications*, vol. 16, no. 3, pp. 398–402, Jun. 1968. DOI: 10.1109/TCOM.1968.1089859.

[18] S. Lin and E. J. Weldon, "Further Results on Cyclic Product Codes", *IEEE Transactions on Information Theory*, vol. 16, no. 4, pp. 452–459, Jul. 1970. DOI: 10.1109/TIT.1970.1054491.

[19] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Co., Jun. 1988.

[20] A. Zeh, A. Wachter-Zeh, and S. V. Bezzateev, "Decoding Cyclic Codes up to a New Bound on the Minimum Distance", *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3951–3960, Jun. 2012. DOI: 10.1109/TIT.2012.2185924.

[21] A. Zeh and S. Bezzateev, "A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes", *Designs, Codes and Cryptography*, pp. 1–18, Jul. 2012. DOI: 10.1007/s10623-012-9721-3.